Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1494

Vragen van het lid **Oosenbrug** (PvdA) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en voor Wonen en Rijksdienst over *langdurige onbereikbaarheid van overheidswebsites* (ingezonden 12 februari 2015).

Antwoord van Minister **Blok** (Wonen en Rijksdienst) mede namens de Minister-President en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie (ontvangen 9 maart 2015)

Vraag 1
Is het waar dat op 10 februari 2015 de website www.rijksoverheid.nl meerdere uren onbereikbaar was? Zo ja, welke overheidssites zijn nog meer door deze storing getroffen?

Antwoord 1
Ja. De storing betrof in ieder geval de twee grote websites rijksoverheid.nl en Defensie.nl, die een belangrijke functie hebben in het communiceren van informatie van de rijksoverheid naar het algemeen publiek. Daarnaast zijn diverse kleine websites geraakt, die zijn gericht op de communicatie met specifieke groepen. De websites van Geenstijl en Telfort zijn ook getroffen.

Vraag 2
Waardoor werd deze storing veroorzaakt en waarom duurde deze zolang?

Antwoord 2
De storing werd veroorzaakt door een DDoS aanval. De storing duurde zo lang, omdat deze vanwege de complexiteit door de leverancier in eerste instantie als een technische storing en niet als een DDoS aanval werd beoordeeld. Toen de conclusie was, dat het een DDoS aanval betrof, was deze binnen enkele uren afgeslagen.

Vraag 3
Welke impact heeft deze storing gehad op het werk van de rijksoverheid en op mensen die overheidsinformatie zochten?

Antwoord 3
De impact op medewerkers van de rijksoverheid is beperkt tot medewerkers die voor rijksoverheid.nl of de andere getroffen websites werken. Redacteuren konden gedurende de storing geen informatie op de websites plaatsen. De publieksvoorlichters van het loket «Informatie rijksoverheid» konden

ah-tk-20142015-1494
ISSN 0921 - 7398
’s-Gravenhage 2015

gedurende de storing de website niet als bron gebruiken voor het beantwoorden van vragen per telefoon of e-mail
Mensen die tijdens de storing informatie van de rijksoverheid zochten, hebben hiervoor rijksoverheid.nl of de andere getroffen websites niet kunnen gebruiken. De vragen van mensen die de publieksvoorlichting «Informatie rijksoverheid» hebben gebeld zijn genoteerd. Na het oplossen van de storing zijn alle vragen, afhankelijk van de voorkeur van de vragensteller, per e-mail of telefoon alsnog beantwoord.
Voor informatie, zoals brieven van de ministers aan de Staten-Generaal, is rijksoverheid.nl niet de enige bron. Deze zijn als Kamerstukken bijvoorbeeld ook op de website van de Tweede Kamer te vinden.

Vraag 4
Welke technische maatregelen zijn genomen om te voorkomen dat de centrale informatiesite van de rijksoverheid langdurig onbereikbaar is? Waardoor hebben deze maatregelen niet gewerkt?

Antwoord 4
Voor de site rijksoverheid.nl en de andere getroffen sites van de rijksoverheid is een set aan beveiligingsmaatregelen (inclusief back-up) genomen, die normaliter afdoende is om DDoS aanvallen te weerstaan of binnen korte tijd op te lossen. Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek. Heel 2014 had rijksoverheid.nl een uitval van 0%. Echter, in dit geval is dit niet afdoende gebleken omdat de leverancier eerst aan een andere oorzaak van de storing dacht (zoals in vraag 2 is vermeld).

Vraag 5
Wat voor acties overweegt u om een urenlange onbereikbaarheid van de website van de rijksoverheid in de toekomst te voorkomen?

Antwoord 5
De leverancier zal een verbeterplan opstellen, waarbij het Ministerie van Algemene Zaken en het Nationaal Cyber Security Centrum (NCSC) nauw betrokken zijn. De analysemethode zal daarvan onderdeel zijn.
Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen Het gaat erom om tegen aanvaardbare kosten de risico's zo minimaal mogelijk te maken.

Vraag 6
Worden voor dienstverlenende overheidswebsites waarbij onbereikbaarheid een zeer grote impact heeft, zoals de Rijksdienst voor het Wegverkeer (RDW) of de Belastingdienst, extra technische maatregelen genomen om de bereikbaarheid te waarborgen? Zo ja, welke? Hadden die deze storing kunnen voorkomen of verkorten? Zo nee, waarom niet?

Antwoord 6
Zowel de RDW als de Belastingsdienst hebben beveiligingsmaatregelen genomen om DDoS aanvallen te weerstaan of binnen korte te tijd af te slaan, een zg. anti-DDoS wasstraat, die verschillende technieken omvat. Zij hebben geen last van deze DDoS aanval gehad. De DDoS aanvallen zijn de laatste tijd tot nu toe zonder al te veel problemen voor de bereikbaarheid afgeweerd.
Het NCSC ondersteunt de overheid en de vitale sectoren onder andere door nieuwe beschikbare informatie over cyberaanvallen te delen met de overheidsorganisaties om er lering uit te trekken en te bezien of (nieuwe) extra maatregelen moeten worden genomen.
Gezien de rapportage van de leverancier zelf (zie vraag 2) heeft de duur van de storing niet gelegen aan de beveiligingsmaatregelen, maar aan de analyse van de storing.